



Wireless 300N PCI Adapter

Model # AWLH6090

User's Manual

Rev. 1.0

Table of Contents

1. Introduction	3
1.1 Package Contents	3
1.2 Features	3
2. Installation	4
3. Configuring the Adapter	13
4. Wireless Monitor.....	18
4.1 Wireless Information	18
4.2 AP List	19
4.3 Profile Settings.....	20
4.4 Configuring Encryption	22
4.5 Ad-hoc and Peer-to-Peer Wireless Networks	28
4.6 Wi-Fi Protected Setup (WPS)	31
4.7 About	36
Appendix A – Features.....	37
Appendix B – Information	38
Industry Canada Statement.....	39
Technical Support	40

1. Introduction

Congratulations on your purchase of the Airlink101® Wireless 300N PCI Adapter. Its high bandwidth combined with extended wireless coverage delivers fast and reliable connection for all of your networking applications when used with other Airlink101® Wireless 300N products.

A full range of security features such as WEP, WPA-PSK, and WPA2-PSK provide the highest level of wireless network security. The bundled Wireless Utility allows you to set up the adapter with an easy-to-use user interface. Best of all the Wireless 300N PCI Adapter works with 802.11g and 802.11b network devices ensuring compatibility with your existing wireless products.

1.1 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

- Wireless 300N PCI Adapter
- Antenna
- Quick Installation Guide
- Installation CD (Driver/Utility/Manual)

1.2 Features

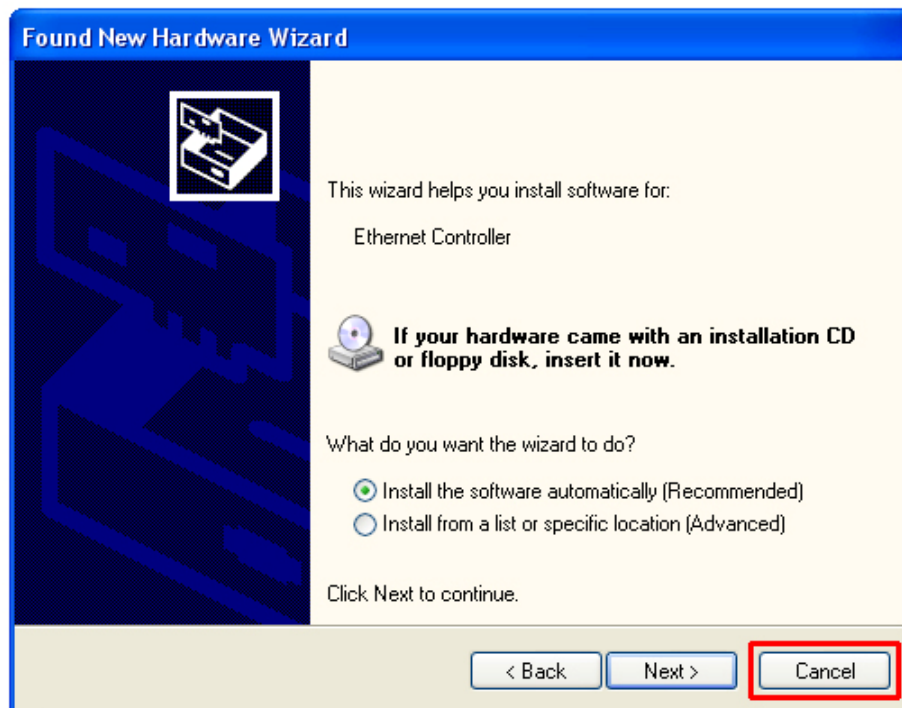
- Industry's highest wireless data rate of up to 300Mbps with IEEE 802.11n draft specification 2.0
- External 3 dipole antennas for wider coverage and continuous connectivity eliminates dead spots
- 64-bit/128-bit WEP encryption, Pre-shared Key (PSK), and Wi-Fi Protected Access (WPA2 and WPA) support provide full protection for your wireless connection
- Higher data rate increases the reliability and stability of wireless connections
- Great for environments with higher wireless data traffic requirements
- Fully backward-compatible with 802.11b/g devices
- Works best with AirLink101® Wireless 300N products

2. Installation

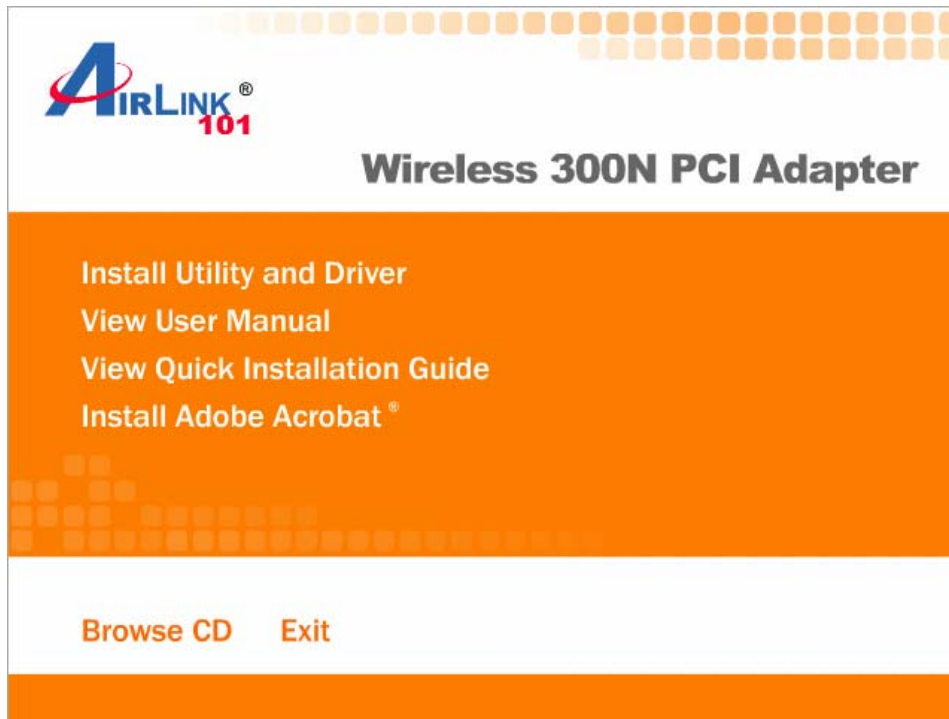
This section provides instructions on how to install the **Wireless 300N PCI Adapter**. The driver is installed along with the utility.

Step 1 Insert the PCI adapter into an available PCI slot, connect the antenna cables firmly to the PCI adapter, and turn on your computer.

Step 2 After turning on the computer, Windows will launch the **Found New Hardware Wizard**. The Found New Hardware Wizard appears differently depending on your operating system. Click **Cancel** to quit the wizard and insert the Installation CD into your CD drive.

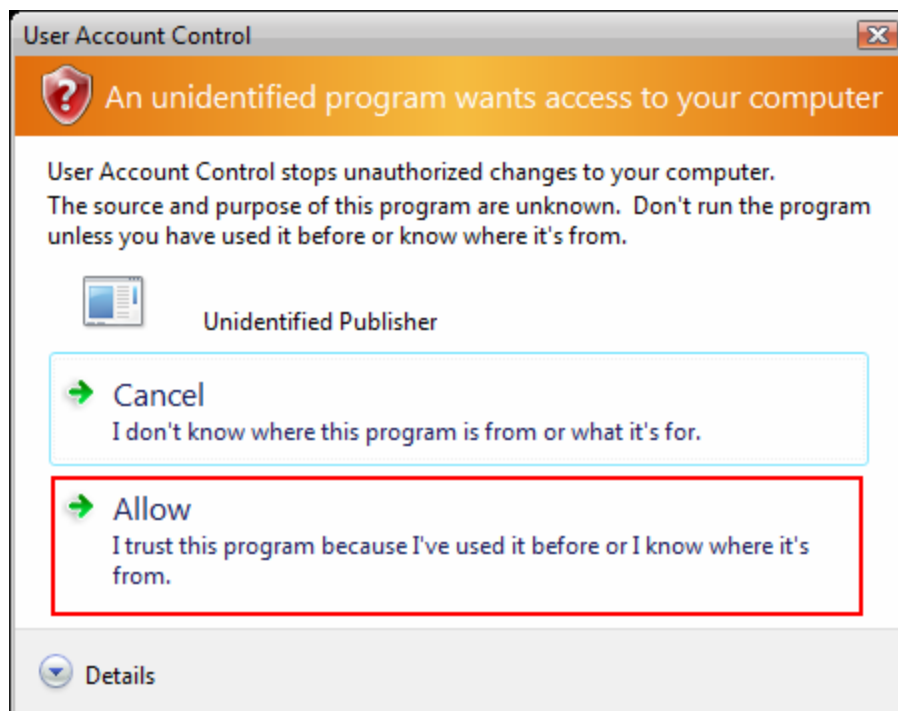


Step 3 The Autorun screen will pop up. Select **Install Utility and Driver** from the menu.

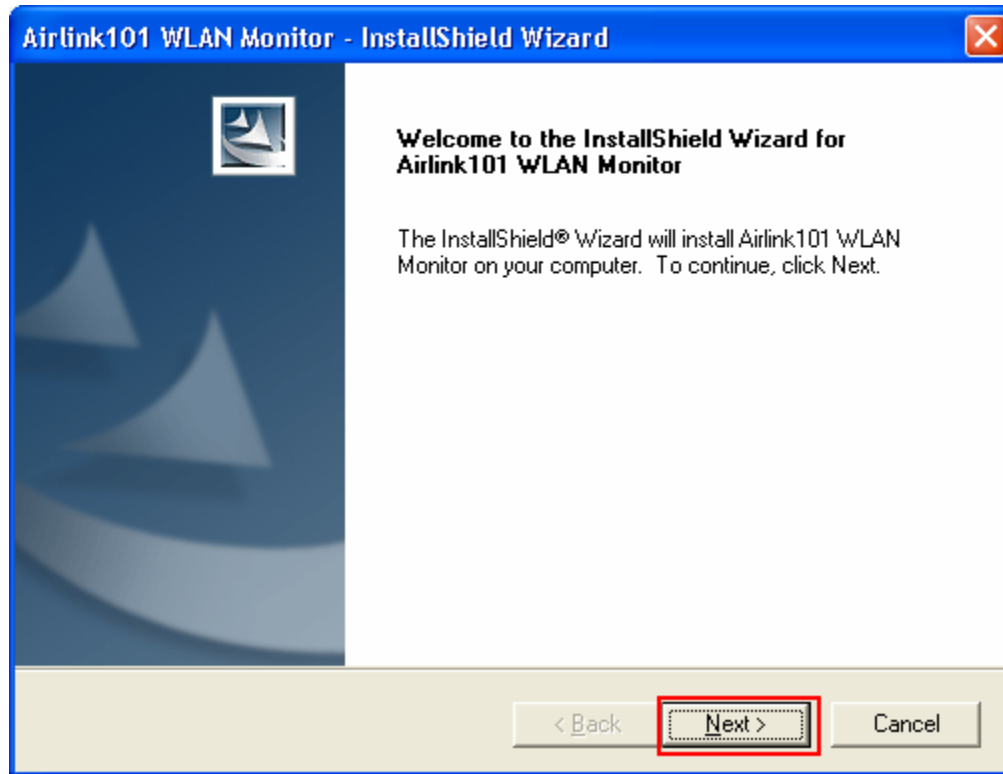


Note: If the Autorun screen doesn't appear automatically, or if you get a blank white screen, go to **Start, Run,** and type **D:\Utility\Setup.exe** (where **D** is the letter of your CD drive) and click **OK**.

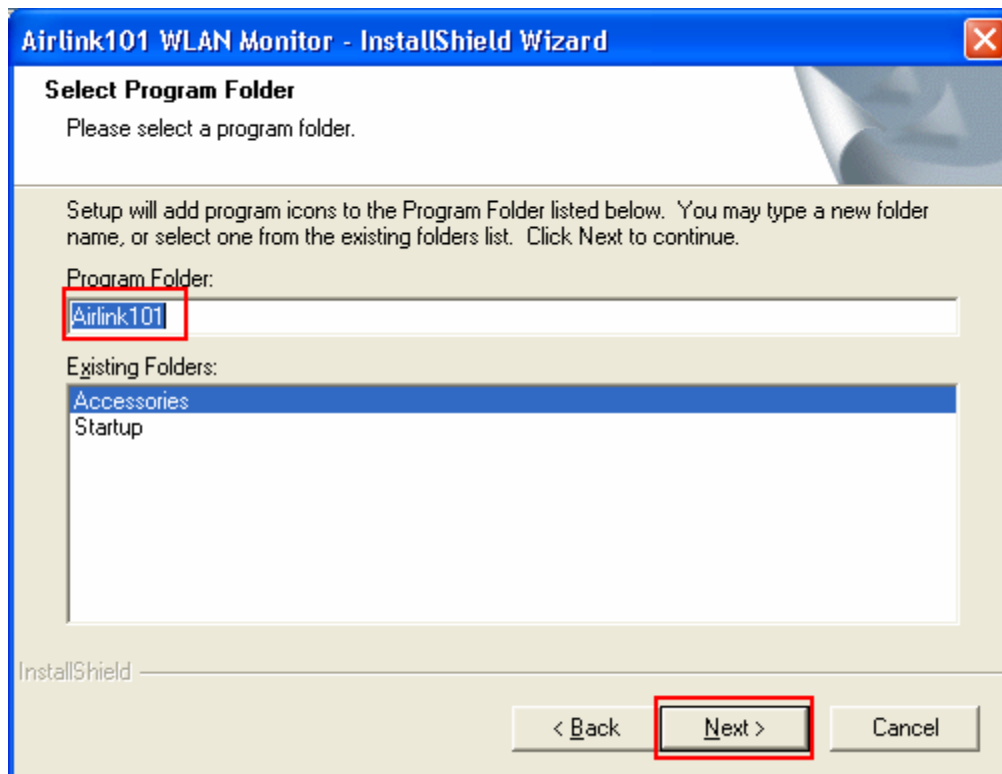
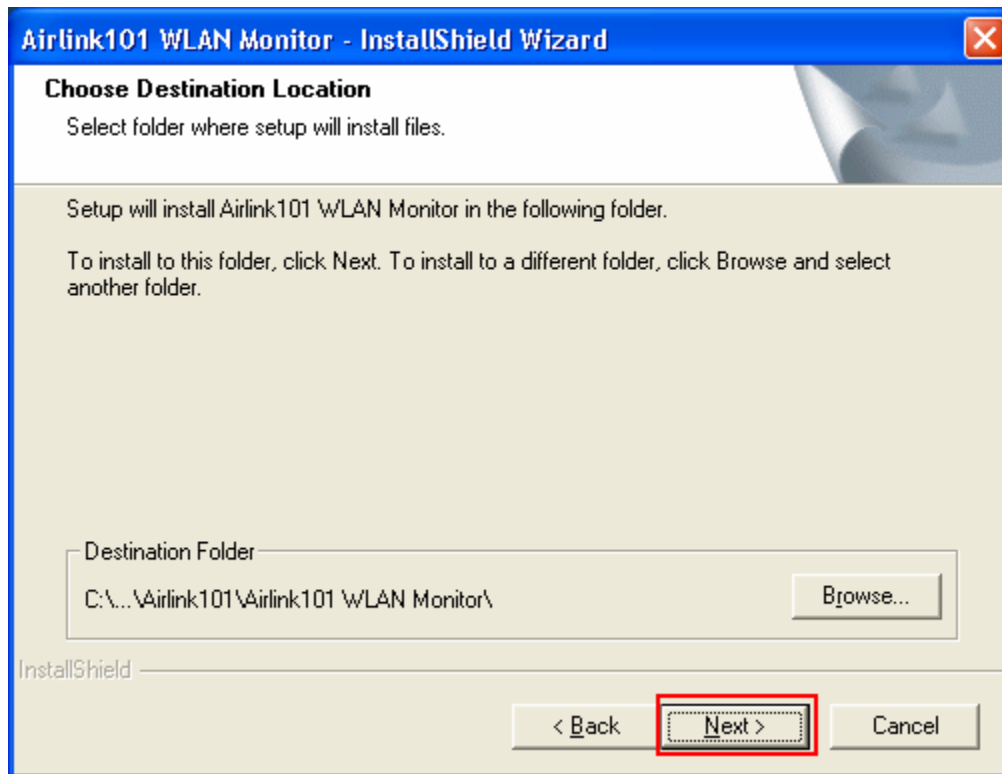
Windows Vista users: At this point, you may get a warning message like the one below. Make sure that you click **Allow** to continue with the installation.



Step 4 Click **Next** at the welcome screen.



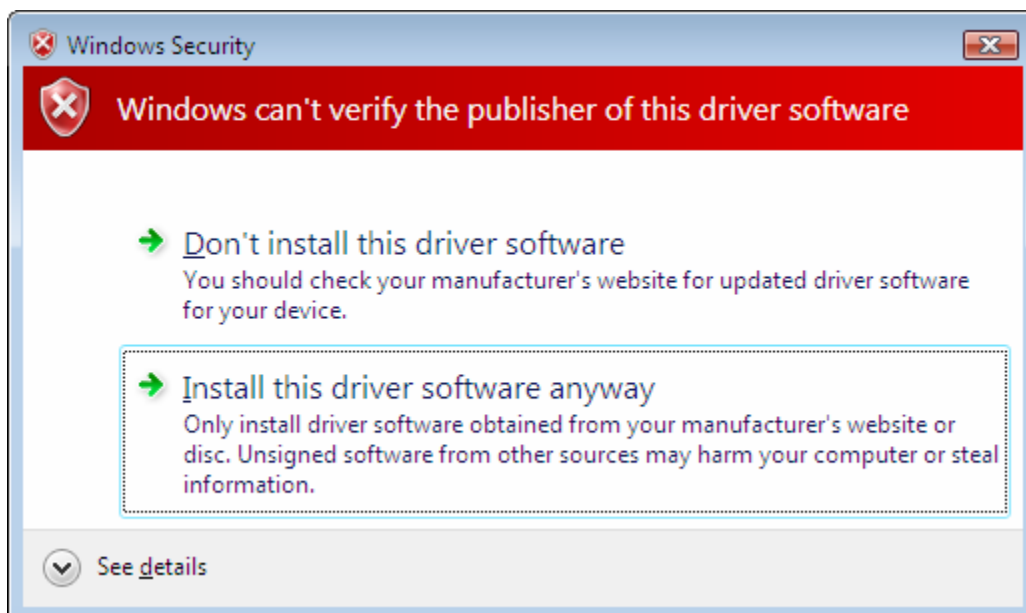
Step 5 Click **Next** to accept the default destination folder.



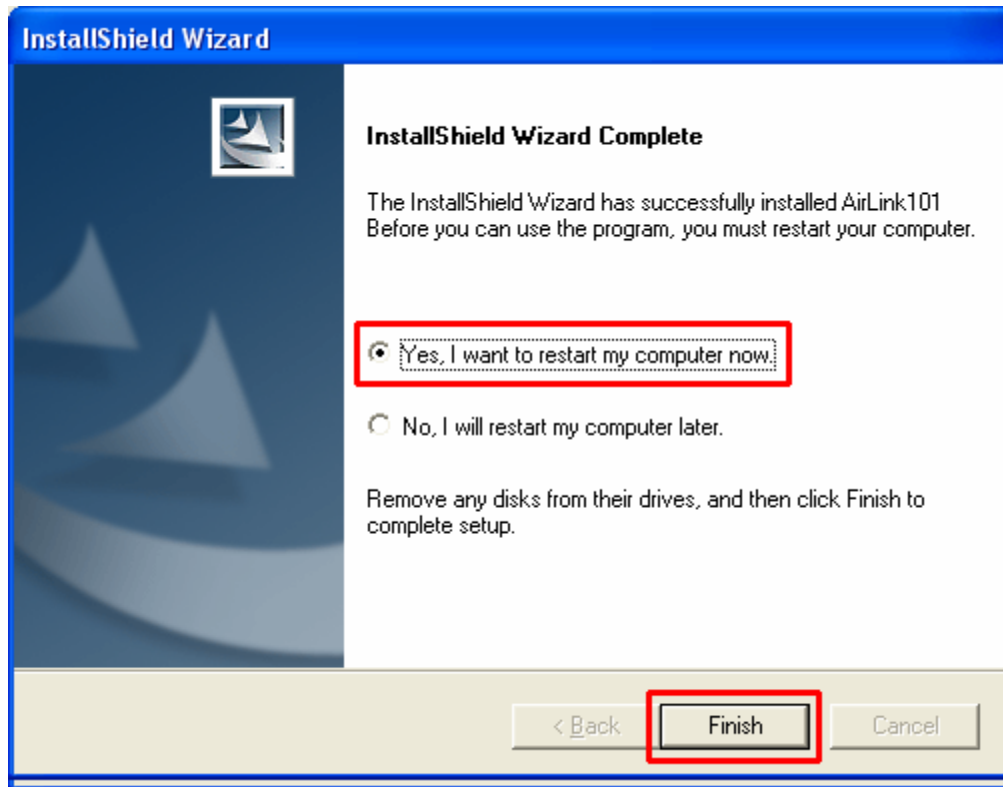
Step 6 Click **Continue Anyway** at the Windows Logo Screen. (For Windows 2000, click **Yes** at the Digital Signature Not Found prompt).



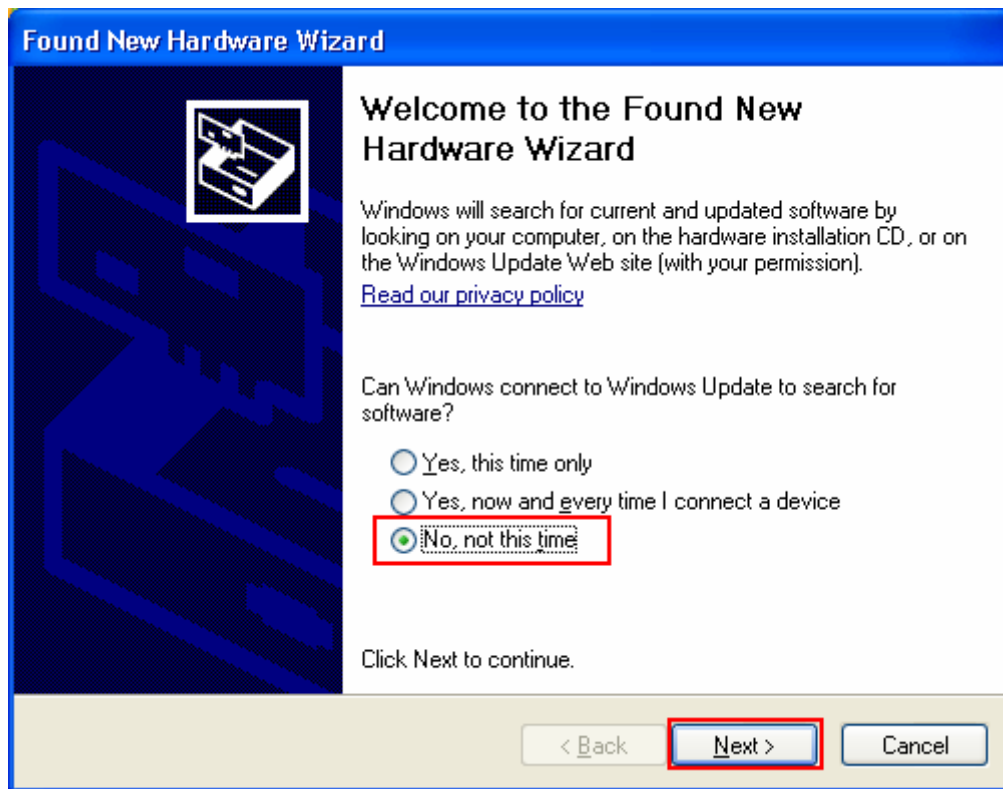
For Windows Vista, click the **Install this driver software anyway** button when the security warning appears.



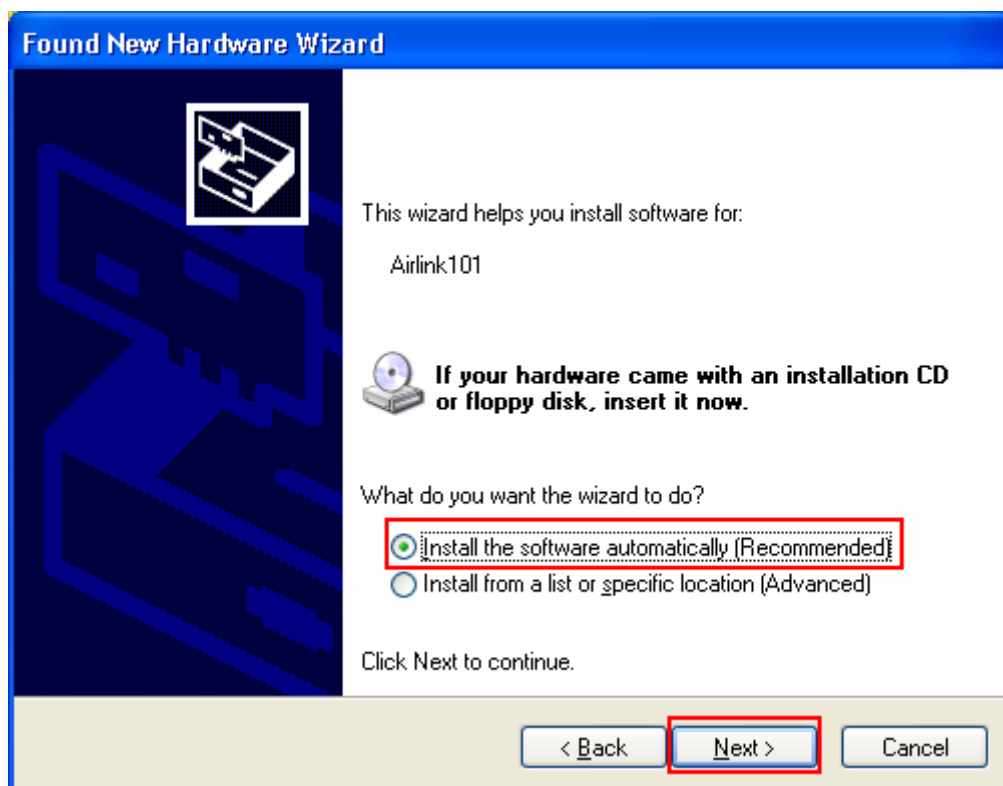
Step 7 Click **Yes, I want to restart my computer now** and then **Finish** to restart your computer.



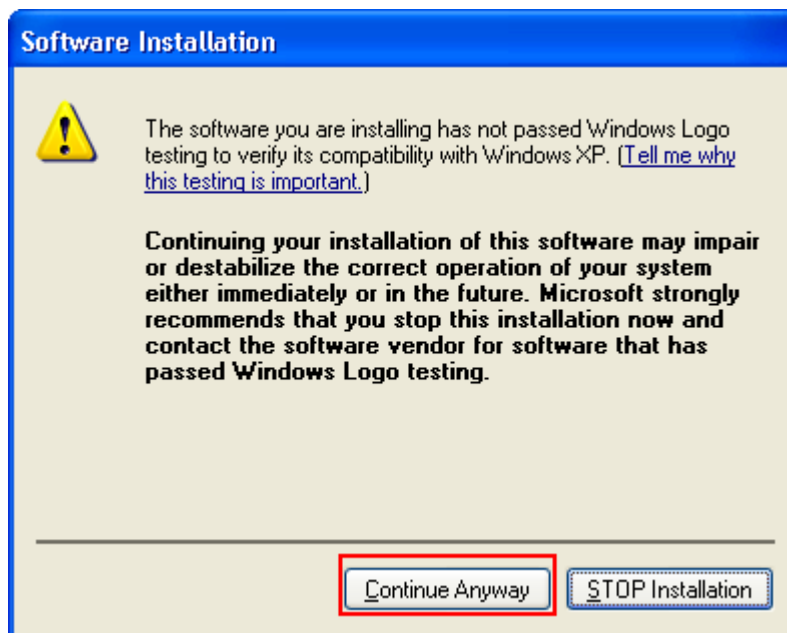
Step 8 After the computer is restarted, Windows will ask to connect to Windows Update, select **No, not this time** and click **Next**. If this screen does not appear, you can skip to section 2.2.



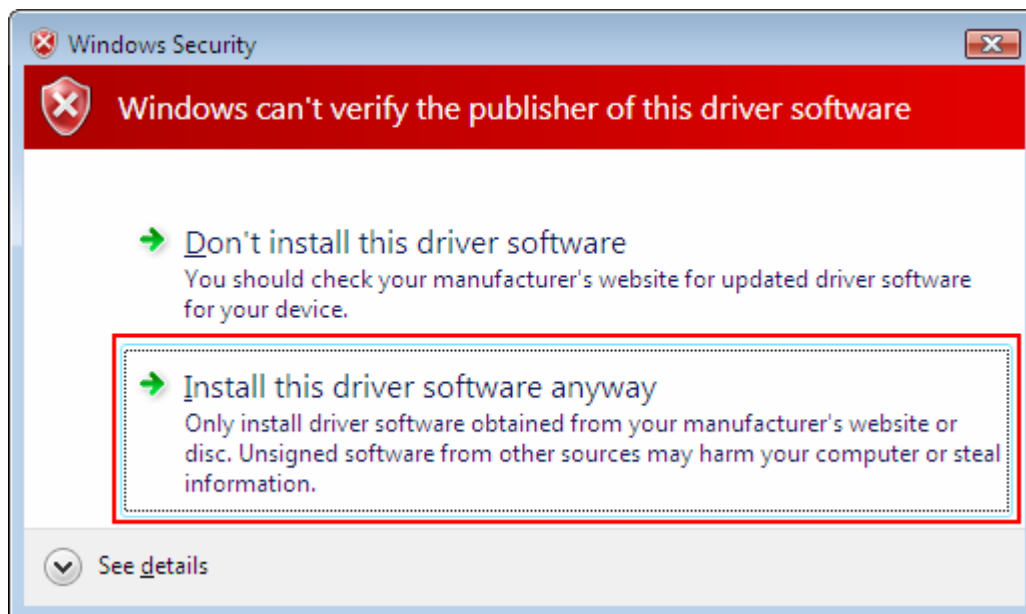
Step 9 Select **Install the software automatically** and click **Next**.



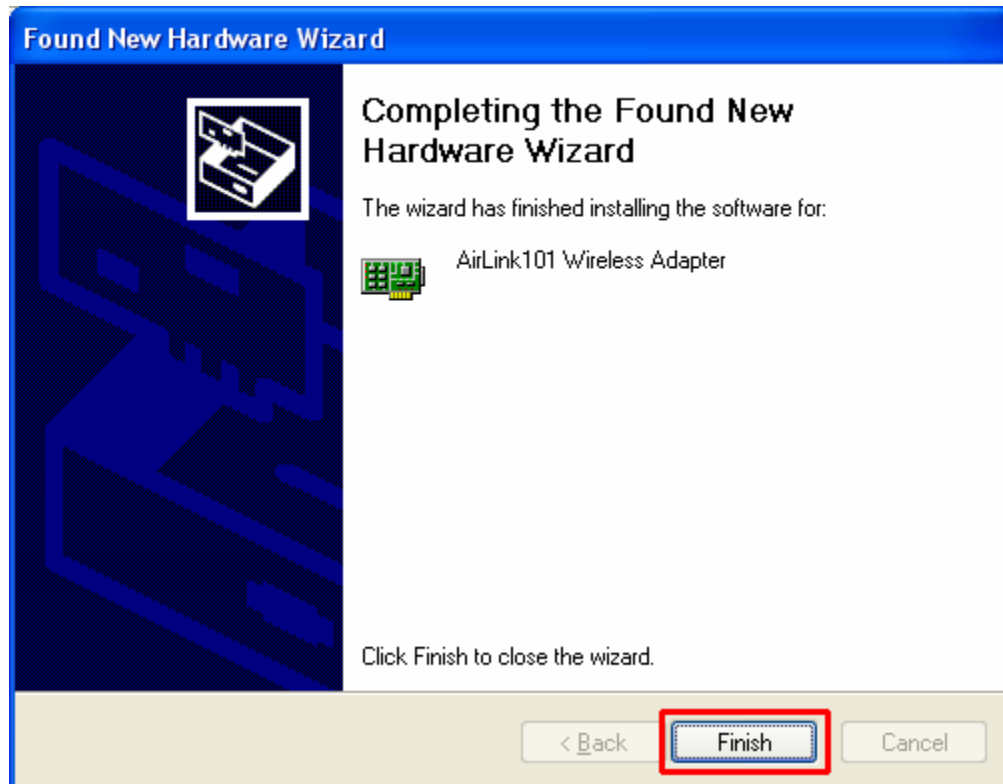
Step 10 Click **Continue Anyway** at the Windows Logo Screen.
(For Windows 2000, click **Yes** at the Digital Signature Not Found prompt).



For Windows Vista, click the **Install this driver software anyway** button when the security warning appears.



Step 11 Click **Finish**.



3. Configuring the Adapter

This section describes how to connect your wireless adapter to a wireless network.

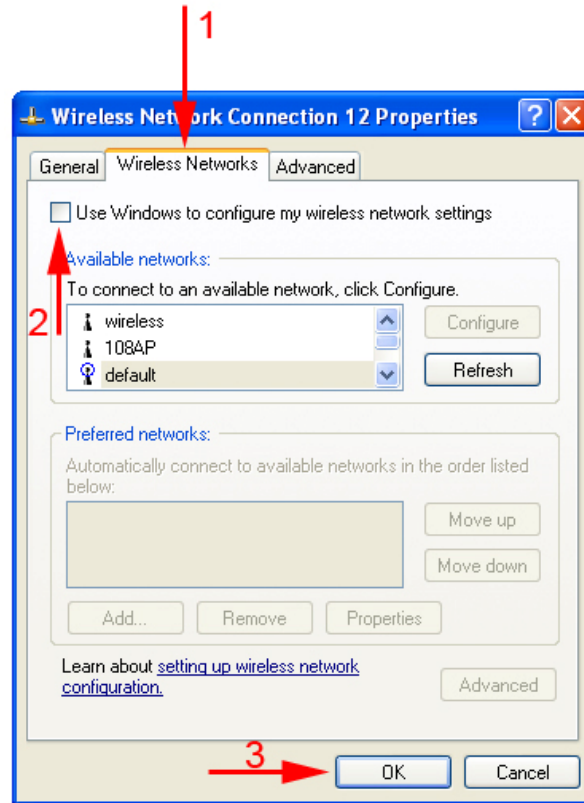
Note to Windows XP Users:

You must disable the Wireless Zero Configuration Utility in order to use the bundled Wireless Utility. Please follow the steps below to disable XP's wireless utility. Windows Vista users can skip the following instructions and go to **Step 1**

Double-click on the **Wireless Network Connection Icon** in the system tray and then click on **Properties** or **Advanced**.



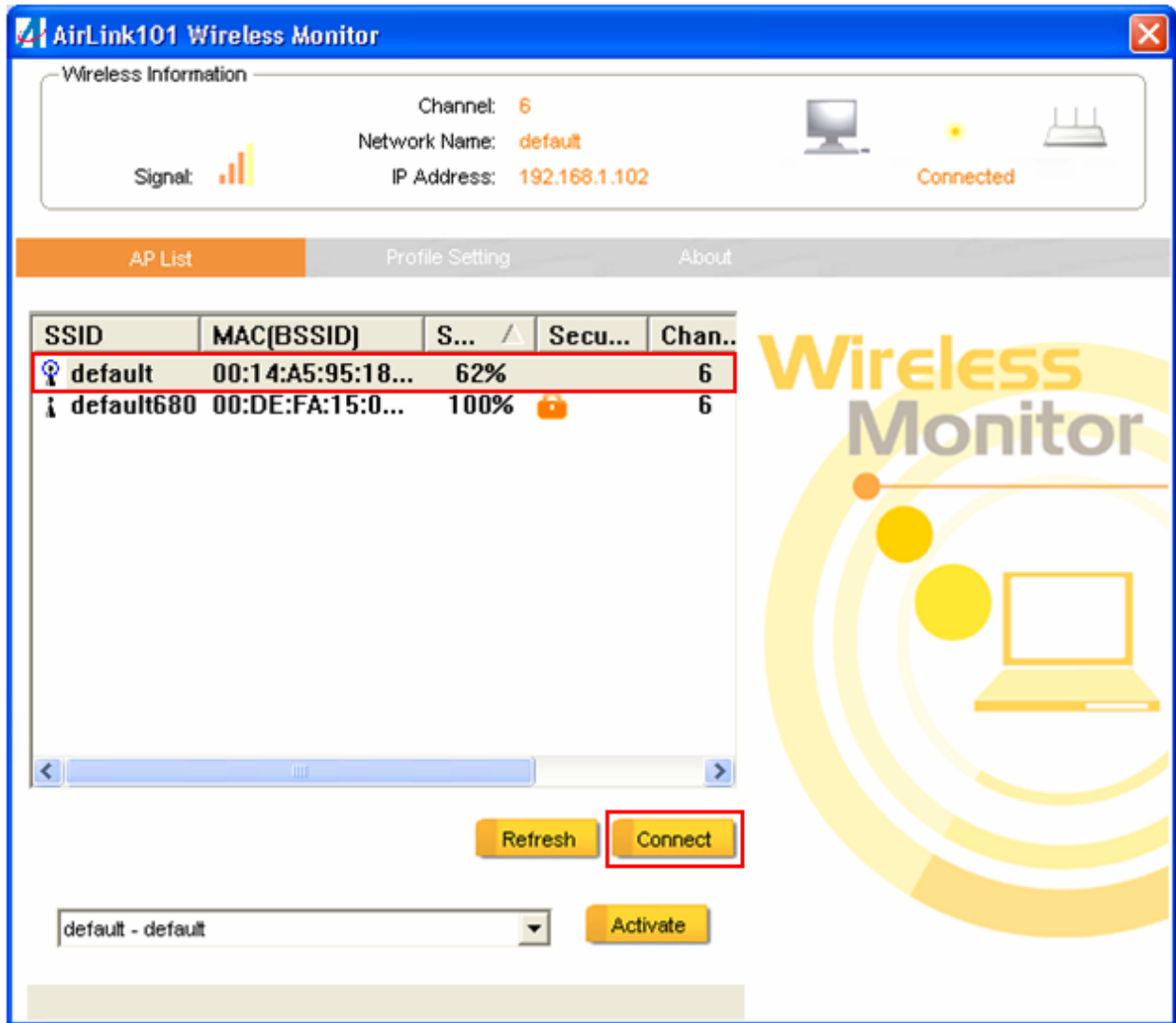
When the new wireless network connection properties window appears, go to the **Wireless Networks** tab, uncheck the “**Use Windows to configure my wireless network settings**” check box and click **OK**.



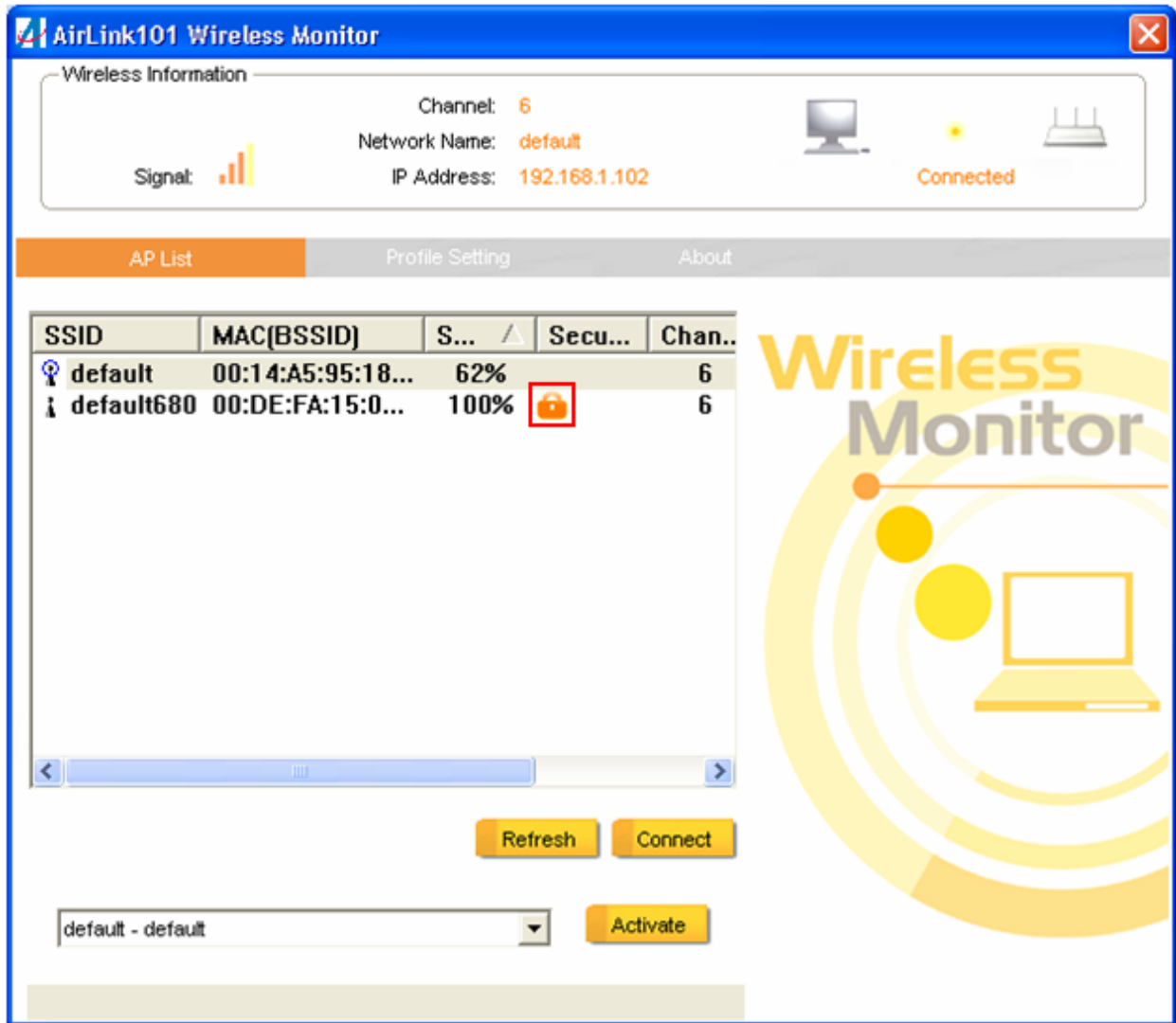
Step 1 To open the utility, double click on the Wireless Monitor icon in the system tray at the bottom right-hand corner of your screen.



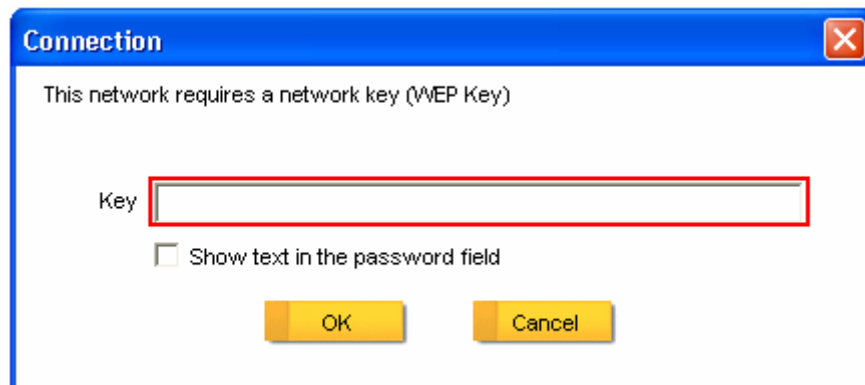
Step 2 Go to the **AP List** tab, select the **SSID** (Network Name) of the wireless network you wish to connect to, and click **Connect**.



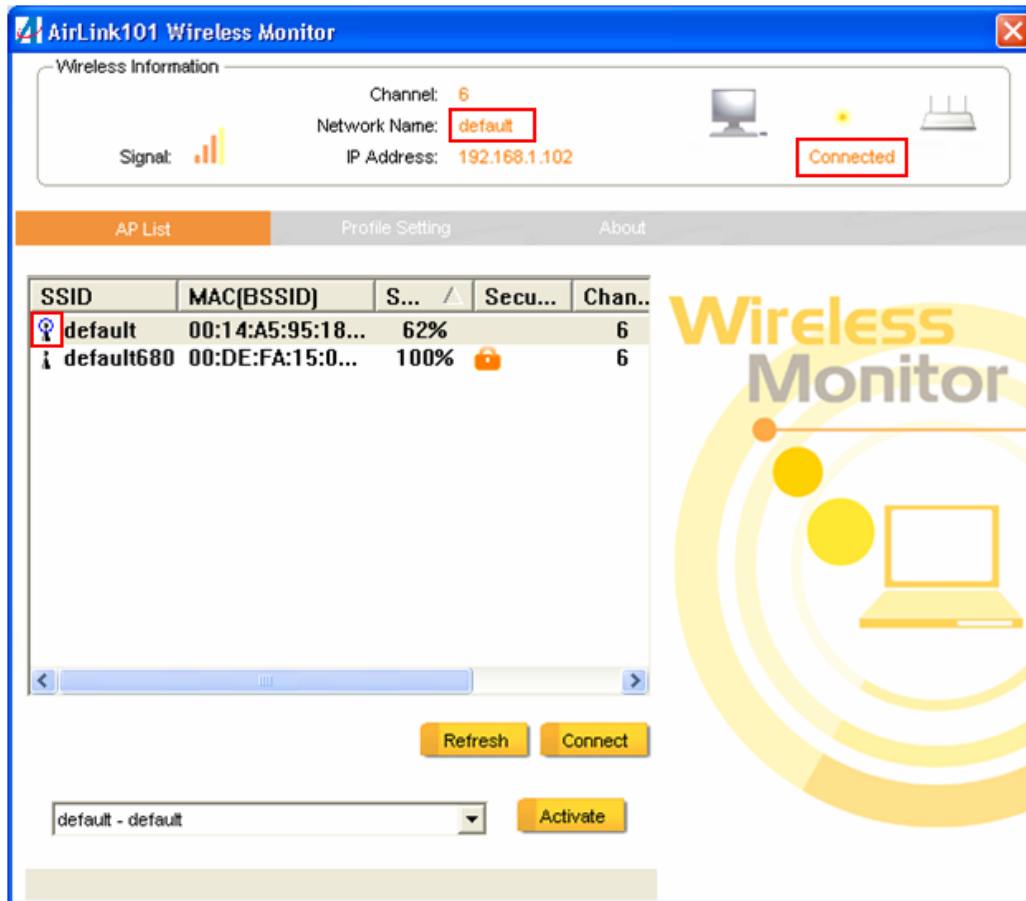
If the network you are attempting to connect to is configured for encryption, you will see an orange lock icon next to the network.



When you click on it and click connect, a box will pop up requesting the wireless encryption key for the router. Enter the encryption key into the box and click **OK**.



Step 3 You should now be connected. You should see “Connected” in the top, right hand corner, and there will be a blue circle around the antenna icon next to the network name.



Troubleshooting: If you are experiencing problems with the connection (unable to connect, low signal strength, slow connection speed, not working, unstable wireless connection) you will want to tune your router’s signal by changing channels on the router.

You do not need to change the channel on the card, it will automatically pick up the new channel after you reboot. The only channel that you need to change is the router’s channel.

Your router has 11 different channels to choose from. Start with channel 1 and work your way up. Each time you change the channel on the router, make sure that you restart the wireless computer before trying to connect again. Keep going through the channels until you find one that gives you a stable connection.

For instructions on changing channels, refer to the documentation that came with your router.

4. Wireless Monitor

This section describes the various functions of the Wireless Monitor that you can configure, including the settings of wireless encryption.

4.1 Wireless Information

The **Wireless Information** box at the top of the window provides you with the status of the current connection, including signal, network name (SSID), IP Address and router channel.

Wireless Information

Channel: 6
Network Name: default
IP Address: 192.168.1.102
Connected

AP List Profile Setting About

SSID	MAC(BSSID)	S... /	Secu...	Chan..
default	00:14:A5:95:18...	62%		6
default680	00:DE:FA:15:0...	100%	🔒	6

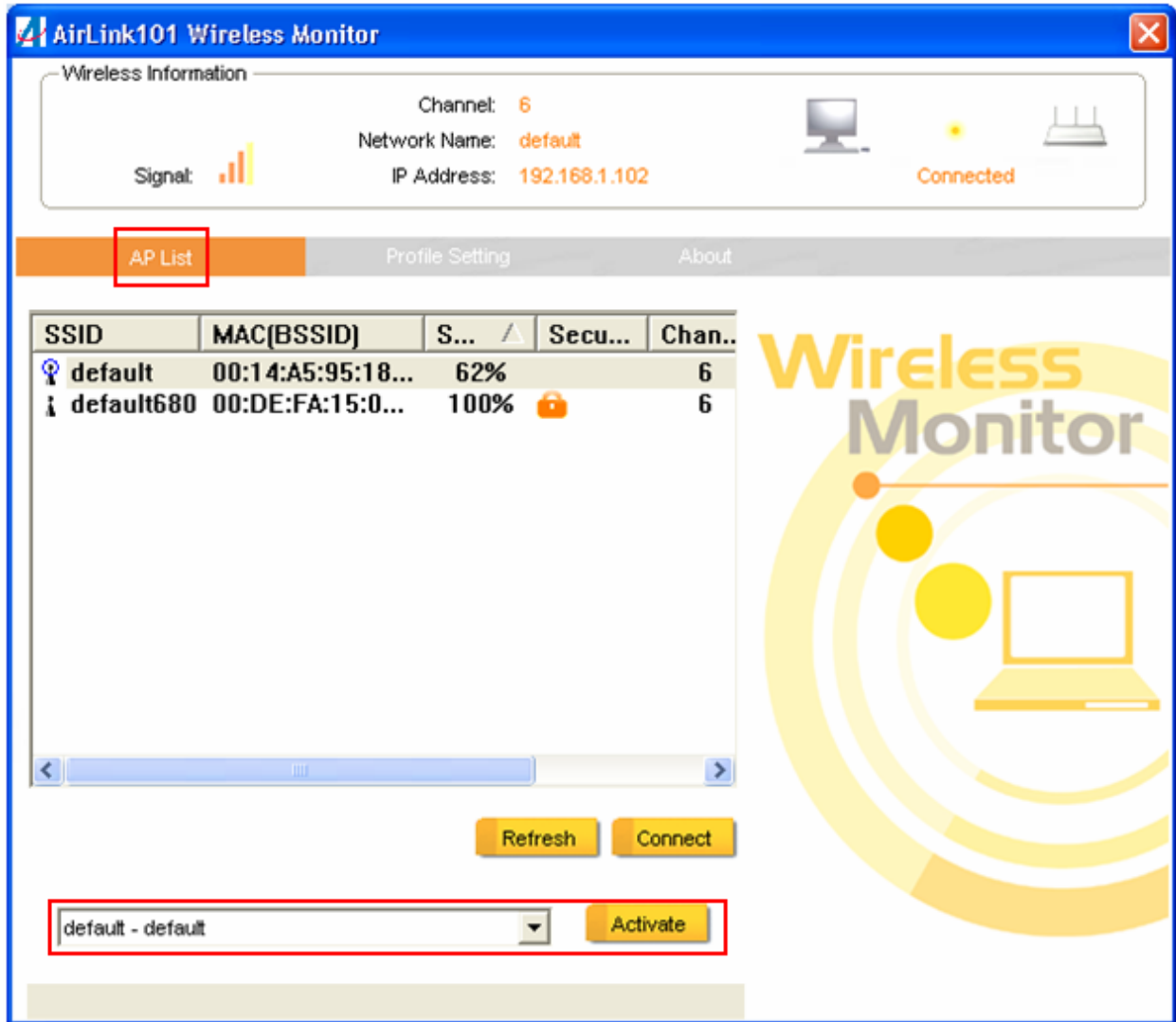
Refresh Connect

default - default Activate

Wireless Monitor

4.2 AP List

The **AP List** tab displays all the available wireless networks detected by the Wireless Adapter. Simply select the wireless network you wish to connect to and click **Connect**. If you have created multiple profiles, you can use the profile chooser at the bottom to select the specific profile you want to use. Then click **Activate** to enable that profile.



4.3 Profile Settings

This section provides instructions on using the **Profile Settings** section of the wireless monitor.

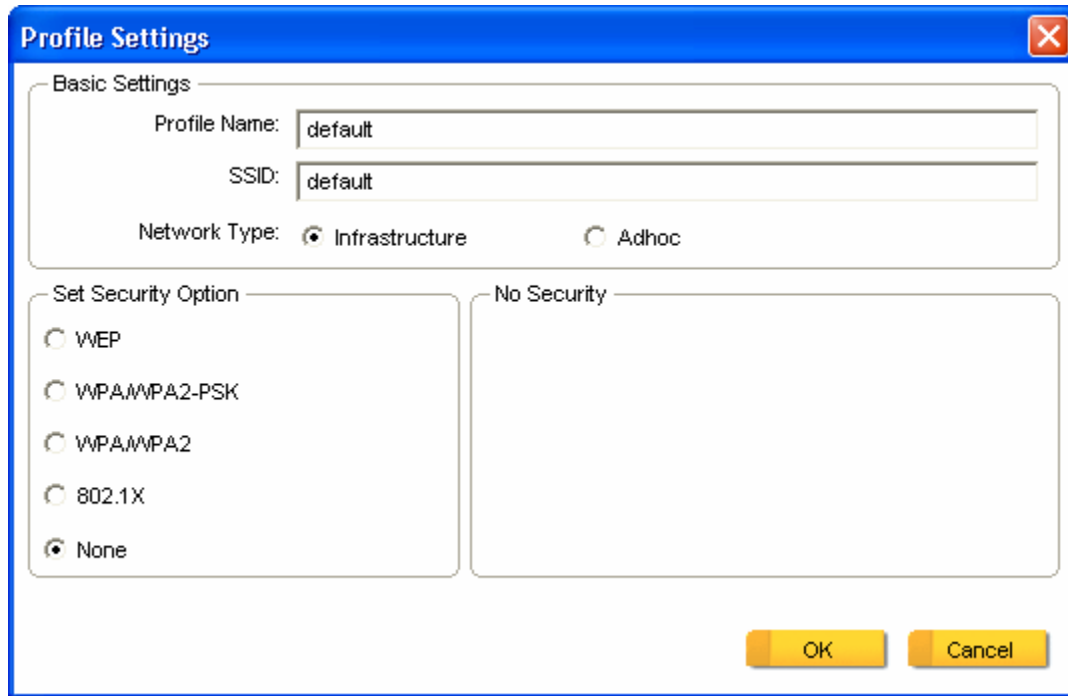


The **My Wireless Networks** box lists the different profiles you've created for the different networks that you use. Profiles are automatically created and added to this list when you connect to new networks. You can also manually add profiles.

To modify an existing profile, select that profile from the **My Wireless Networks** box and click on modify.

To create a new profile, click on **New**.

The **Profile Settings** box will appear allowing you to specify the settings for your new profile or change settings for your existing profile.



The image shows a 'Profile Settings' dialog box with a blue title bar and a close button in the top right corner. The dialog is divided into two main sections. The top section, titled 'Basic Settings', contains two text input fields: 'Profile Name' with the value 'default' and 'SSID' with the value 'default'. Below these fields are two radio buttons for 'Network Type': 'Infrastructure' (which is selected) and 'Adhoc'. The bottom section is split into two panes. The left pane, titled 'Set Security Option', contains five radio buttons: 'WEP', 'WPA/WPA2-PSK', 'WPA/WPA2', '802.1X', and 'None' (which is selected). The right pane, titled 'No Security', is currently empty. At the bottom right of the dialog are two yellow buttons labeled 'OK' and 'Cancel'.

Once you are finished entering the settings, click **OK** to save the changes.

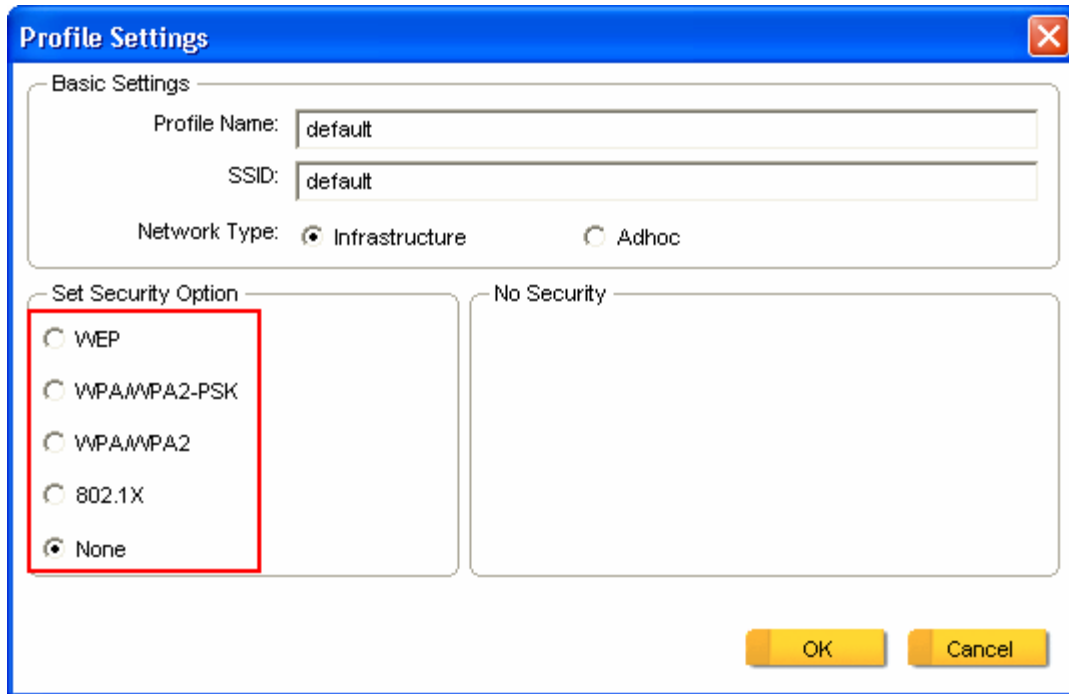
4.4 Configuring Encryption

This section describes the different types of encryption available and how to configure them. In most cases, encryption will be automatically configured and all that will need to be entered is the key, as described in **Section 3 Step 2**. The only time you will need to manually configure the encryption settings is if you are creating a custom profile.

Click on **Profile Settings** then **New**.



The profile settings box will appear. This is where you will change your encryption settings. As you can see you have five different options to choose from.



These three are meant for the home user:

None: No encryption in use

WEP: The most popular but least secure form of encryption

WPA/WPA2-PSK: The most secure and recommended level of encryption

The remaining two are for use in a corporate environment that utilizes authentication servers. If you do not know if you have an authentication server, you probably don't and will want to stick with the three options above.

Configuring WEP encryption

The screenshot shows a 'Profile Settings' dialog box with a blue title bar and a close button in the top right corner. It is divided into three main sections:

- Basic Settings:** Contains text input fields for 'Profile Name' and 'SSID'. Below them, 'Network Type' has two radio buttons: 'Infrastructure' (which is selected) and 'Adhoc'.
- Set Security Option:** A group box containing five radio buttons: 'WEP' (selected and highlighted with a red box), 'WPA,WPA2-PSK', 'WPA,WPA2', '802.1X', and 'None'.
- Wired Equivalent Privacy(WEP):** A group box containing three radio buttons: 'Open' (selected), 'Shared' (highlighted with a red box), and 'Auto'. Below these is a 'Key:' text input field. Further down are two dropdown menus: 'Key Length:' (set to '64 bits (40+24) - 10 Hexadeci' and highlighted with a red box) and 'Key Index:' (set to '1' and highlighted with a red box). At the bottom of this section is a checkbox labeled 'Show text in the password field' which is currently unchecked.

At the bottom right of the dialog are two yellow buttons: 'OK' and 'Cancel'.

Select **WEP** from the **Set Security Option** box.

Under **Wired Equivalent Privacy (WEP)**, you will want to select **Shared** or **Open**, depending on the router settings.

In the **Key** box, you will want to type in the encryption key for the router. If you check the **Show text in the password field** box, your key will appear in the box as you are typing it instead of showing only asterisks. This is helpful as it allows you to double check the key before saving the changes.

Key Length will also be predetermined by the router. Refer to your routers settings to find out what you should select here.

Key Index is the key on the router that is currently in use. Refer to your routers settings to find out what you should choose.

Once you are done, click **OK** to save your settings.

Configuring WPA/WPA2-PSK Encryption (for home users)

The screenshot shows a 'Profile Settings' dialog box with the following sections:

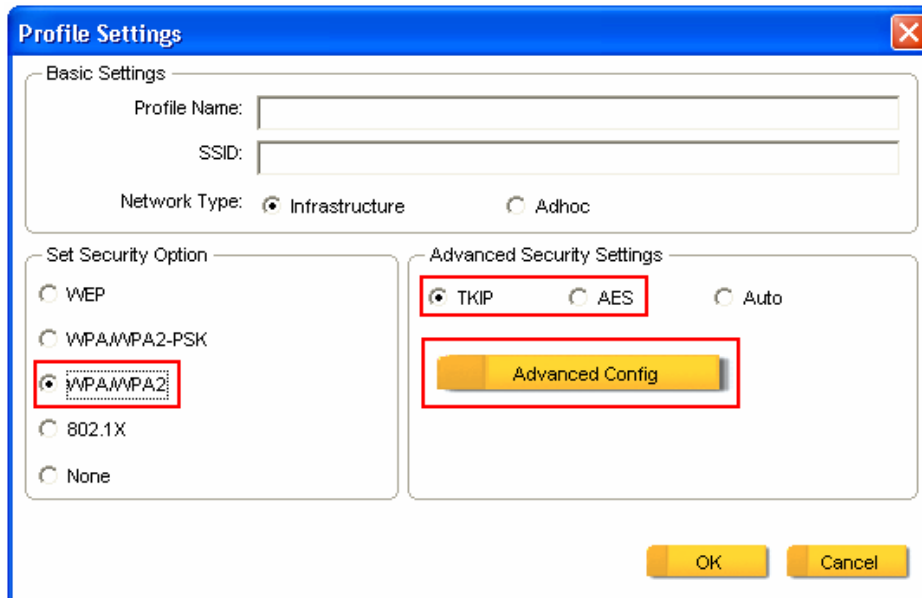
- Basic Settings:** Profile Name: [text box], SSID: [text box], Network Type: Infrastructure Adhoc
- Set Security Option:** WEP, WPA/WPA2-PSK, WPA/WPA2, 802.1X, None
- Passphrase Settings:** TKIP AES Auto, Key: [text box]
- Show text in the password field
- Buttons: OK, Cancel

Select **WPA/WPA2-PSK** from the **Set Security Option** box.

Under **Passphrase Settings** select either **TKIP** or **AES** depending on the settings for your router.

Enter the encryption key into the **KEY** box.

Configuring WPA/WPA2 Encryption (for corporate networks)



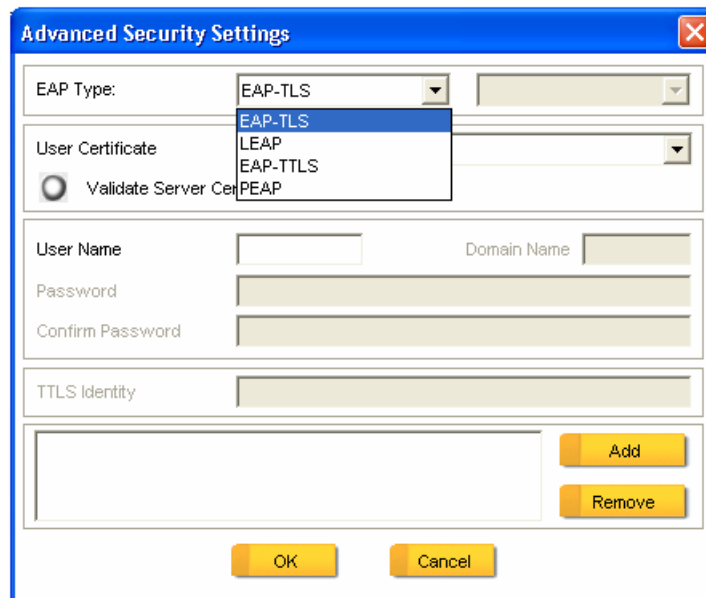
The screenshot shows the 'Profile Settings' dialog box. It is divided into several sections:

- Basic Settings:** Includes fields for 'Profile Name' and 'SSID', and radio buttons for 'Network Type' (Infrastructure selected, Adhoc unselected).
- Set Security Option:** A group of radio buttons with 'WPA/WPA2' selected. Other options include WEP, WPA/WPA2-PSK, 802.1X, and None.
- Advanced Security Settings:** Includes radio buttons for 'TKIP' (selected), 'AES', and 'Auto'. Below these is a yellow 'Advanced Config' button.
- Buttons:** 'OK' and 'Cancel' buttons are located at the bottom right.

Select **WPA/WPA2** from the **Set Security Option** box.

Under **Advanced Security Settings** select either **TKIP** or **AES** depending on the settings for your router.

Click on **Advanced Config** to enter your authentication settings.

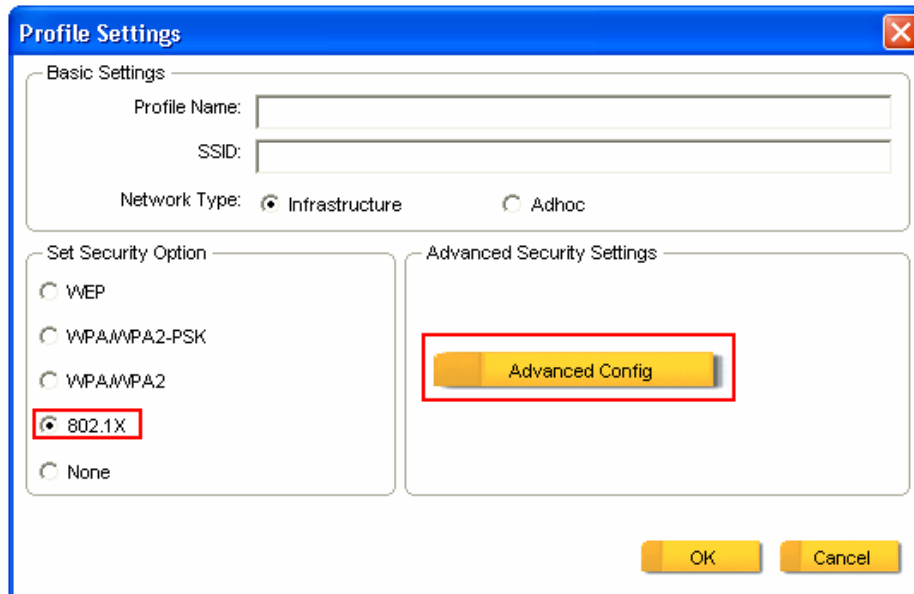


The screenshot shows the 'Advanced Security Settings' dialog box. It contains the following fields and controls:

- EAP Type:** A dropdown menu with 'EAP-TLS' selected. A list of options is shown: EAP-TLS, LEAP, EAP-TTLS, and PEAP.
- User Certificate:** A dropdown menu.
- Validate Server Certificate:** A checked radio button.
- User Name:** A text input field.
- Domain Name:** A text input field.
- Password:** A text input field.
- Confirm Password:** A text input field.
- TTLS Identity:** A text input field.
- Buttons:** 'Add' and 'Remove' buttons are on the right side of the TTLS Identity field. 'OK' and 'Cancel' buttons are at the bottom.

The adapter supports EAP-TLS, LEAP, EAP-TTLS, and PEAP authentication methods. Refer to your system administrator for information about what settings you should enter here.

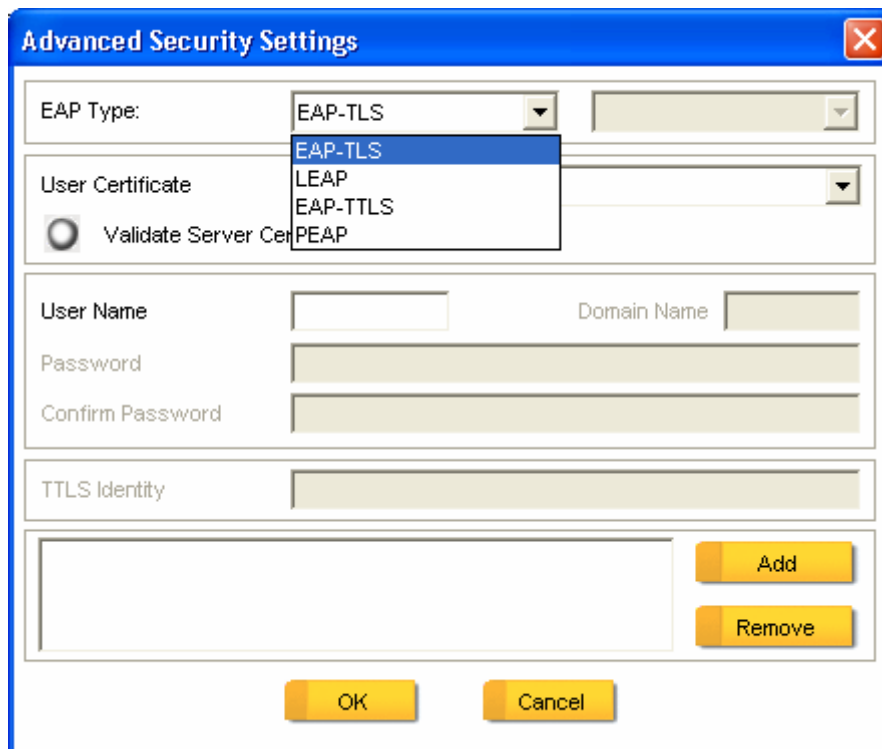
Configuring 802.1x authentication (for corporate networks)



The screenshot shows the 'Profile Settings' dialog box. It is divided into two main sections: 'Basic Settings' and 'Advanced Security Settings'. In the 'Basic Settings' section, there are fields for 'Profile Name' and 'SSID', and radio buttons for 'Network Type' with 'Infrastructure' selected. In the 'Advanced Security Settings' section, there are radio buttons for 'Set Security Option' with '802.1X' selected. A yellow button labeled 'Advanced Config' is highlighted with a red rectangular box. At the bottom right, there are 'OK' and 'Cancel' buttons.

Select **802.1x** from the **Set Security Option** box.

Click on **Advanced Config** to enter your authentication settings.



The screenshot shows the 'Advanced Security Settings' dialog box. The 'EAP Type' dropdown menu is open, showing a list of options: EAP-TLS, LEAP, EAP-TTLS, and PEAP. The 'Validate Server Certificate' checkbox is checked. There are fields for 'User Name', 'Domain Name', 'Password', and 'Confirm Password'. There is also a 'TTLS Identity' field. At the bottom right, there are 'Add' and 'Remove' buttons. At the bottom center, there are 'OK' and 'Cancel' buttons.

The adapter supports EAP-TLS, LEAP, EAP-TTLS, and PEAP authentication methods. Refer to your system administrator for information about what settings you should enter here.

4.5 Ad-hoc and Peer-to-Peer Wireless Networks

Ad-hoc networking is used when you want to connect two or more computers together but you don't have a router.

In ad-hoc mode, you lose a lot of the features that come with a router. The maximum connection speed drops significantly to 11Mbps. WEP encryption is the only security available in ad-hoc mode.

To set up ad-hoc mode, you will need to create a new profile.



Open the **Wireless Monitor**.

Click on **Profile Setting**, then click on **New**.

The profile settings box will appear.

The screenshot shows a 'Profile Settings' dialog box with the following elements:

- Basic Settings:**
 - Profile Name: [Text Input]
 - SSID: [Text Input]
 - Network Type: Infrastructure, Adhoc
 - Channel: 6 (Dropdown)
- Set Security Option:**
 - WEP
 - None
- No Security:** [Empty Panel]
- Buttons:** OK, Cancel

First change the network type to **Adhoc**. (Infrastructure is for when you are using a router).

Enter a profile name into the **Profile Name** box so that you can identify the profile.

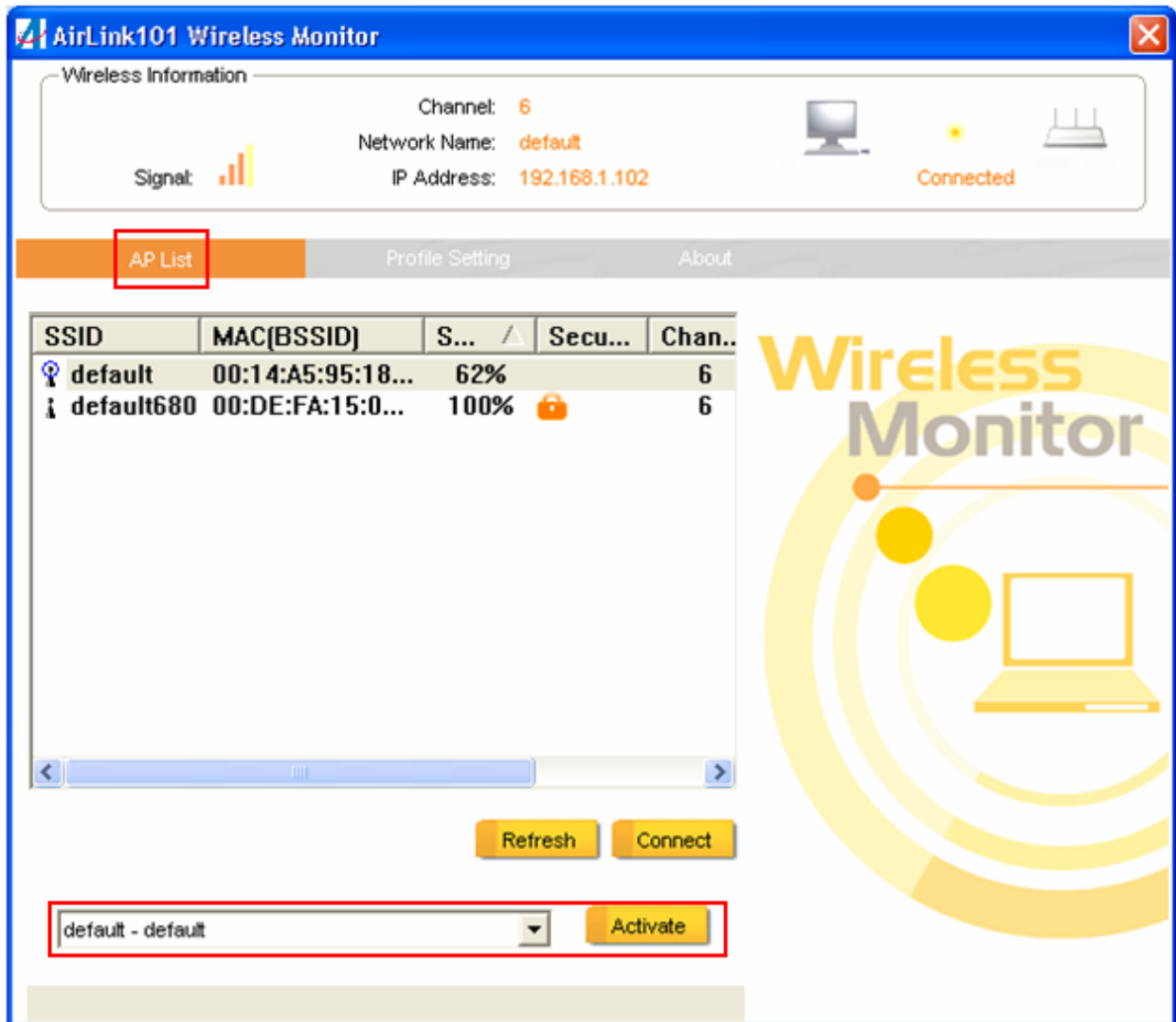
Type in a network name (SSID) into the **SSID** box

Select your desired **Channel**

You can also choose between no security or WEP security. If you choose WEP security, you can follow the instructions in the **Configuring Encryption** section of the manual.

Click **OK** to save the profile.

Once that is done, click on the **AP List**.



Select your new profile from the profile chooser and click **Activate** to enable the profile.

You will need to configure all other computers that you are planning on connecting to your ad-hoc network with the same settings that you input on this screen. Every computer has to be set up exactly the same. If any of the settings are different, the network will not function.

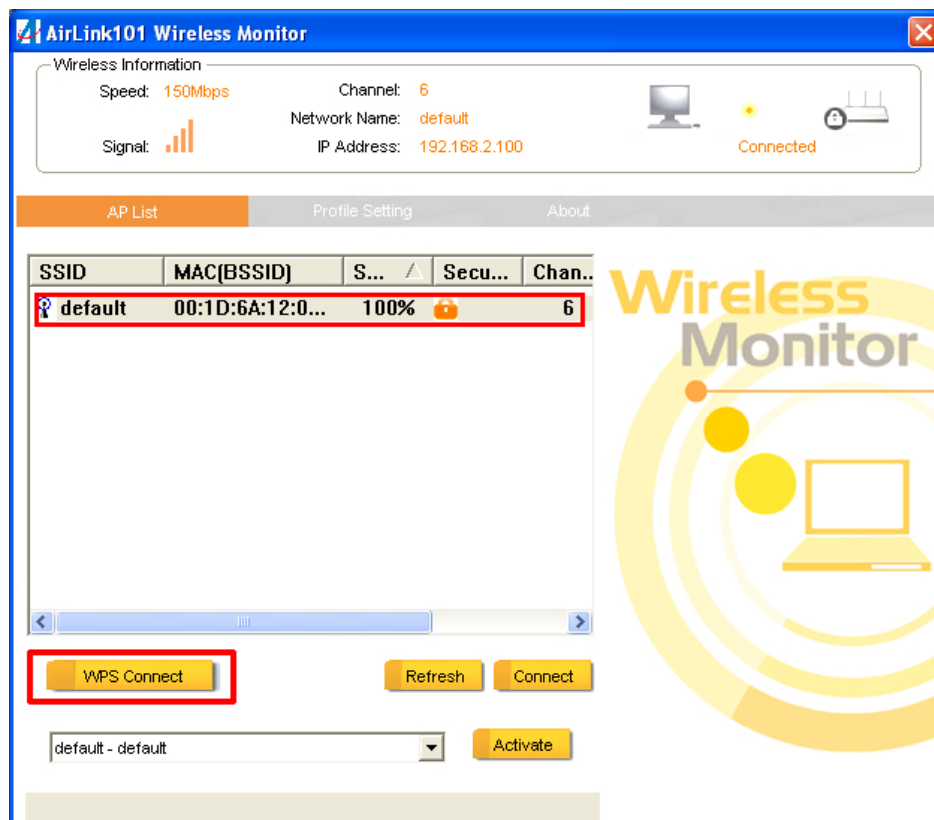
Troubleshooting: If you are having trouble connecting, if the connection is slow, or if it is unstable, you will want to try changing channels. Start with channel 1 and work your way up until you find a channel that gives you a stable connection. Each time you change the channel, save the settings, then reboot the computer. Also make sure that you do this on every ad-hoc machine so that they will all be set to the same channel.

4.6 Wi-Fi Protected Setup (WPS)

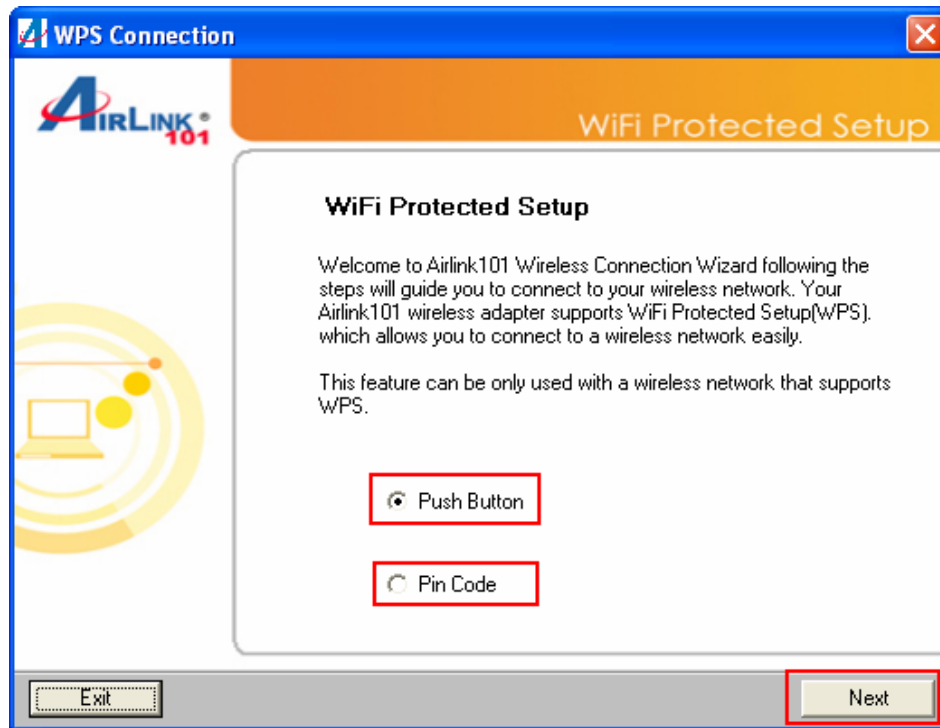
Wi-Fi Protected Setup™ (WPS) is a new and easy way to configure the encryption for your wireless network clients to connect to your router. If your wireless router does not support WPS feature or it is disabled on your router (WPS is disabled when you use WEP as the wireless encryption), you will need to set up the wireless security manually and you can skip this section.

In the instructions below, we are going to use the utility, Wireless Monitor that comes with the Airlink101 Wireless 300N adapters and the AR690W Airlink101 Wireless 300N router as the example.

Step 1 Go to the computer with the Wireless 300N adapter and open the Airlink101 Wireless Monitor. Click on the **WPS Connect** button.



Step 2 Choose your configuration method, either **Push Button** or **Pin Code** and click **Next**.



Step 3a If you choose the Push Button method, make sure that you click on the **Wi-Fi Protected Setup** button.



Step 3b Push the WPS button on the router, and the blue LED will start blinking. The router will now start the handshake with the wireless adapter, then the connection will be built up in couple minutes.



Step 4a If you choose the Pin Code method, write down the **PIN** and click **Next**.



Step 4b Log in to your router's configuration page from the web browser and click on **Wireless**. Then click **Wireless security**. Make sure that the **Wi-Fi Protected Setup Enable** box is checked. Click the **Add Wireless Device Wizard** button.

AIRLINK 101

Setup | **Wireless** | Security | Access Restrictions | Application & Gaming | Administration | Status

300N Wireless Router | Basic Wireless Settings | **Wireless Security** | Wireless MAC Filter | Advanced Wireless Settings

Wireless Network

Wireless Settings

Security Mode: Disabled

Wi-Fi Protected Setup

Enable:

Current PIN: 85282483

Generate New PIN | Reset PIN to Default

Wi-Fi Protected Status: Enabled / Not Configured

Reset to Unconfigured | **Add Wireless Device Wizard**

Apply | Cancel

Step 4c Enter the Pin Code in the **Pin Number** box and click **Connect**.

Draft 802.11N Wireless Router

Wi-Fi Protected Setup

There are two way to add a wireless device to your wireless network: PIN or Push Button.

If the wireless device you want to add only comes with a PIN number, enter its PIN number below and press the "Connect" button. It will help you to add this device to your wireless network.

PIN number : **Connect**

If the wireless device your want to add has both options available, you may use the Virtual Push Button if you prefer.

Push Button :

Back

After a few moments both the router configuration screen and the adapter configuration screen should show a message telling you that you are connected.

Step 4d Click **Continue** on the router configuration screen.

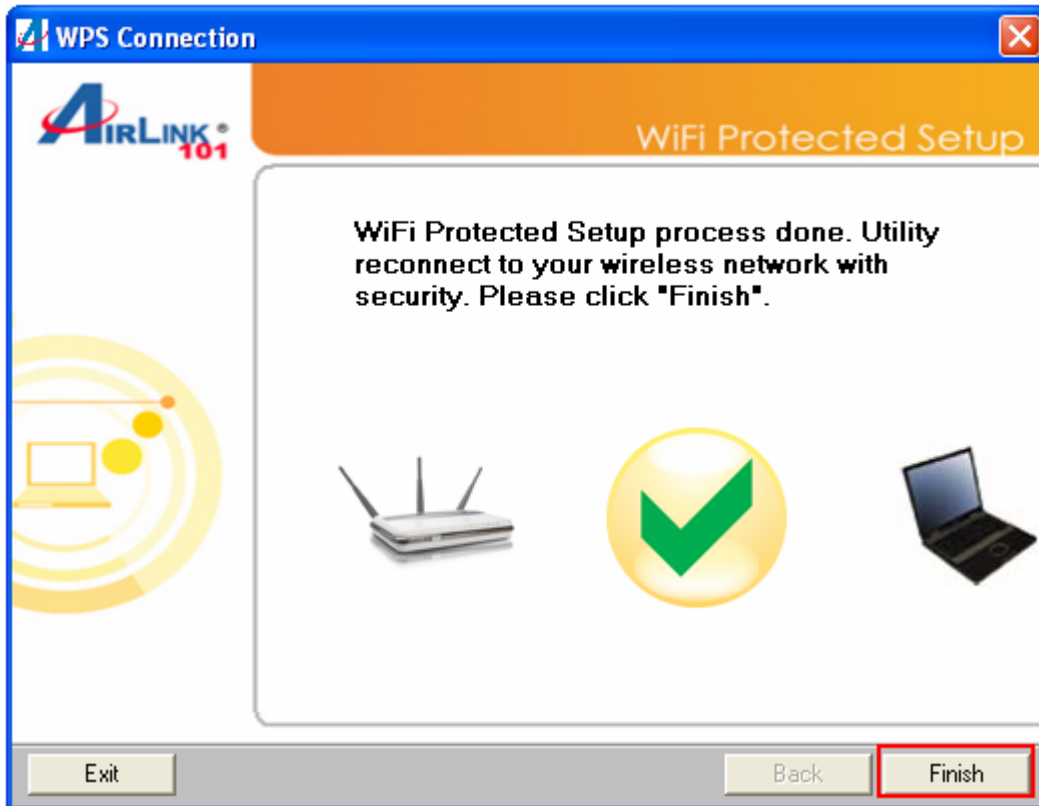
WPS - The Result of Adding Wireless Device

WPS Success

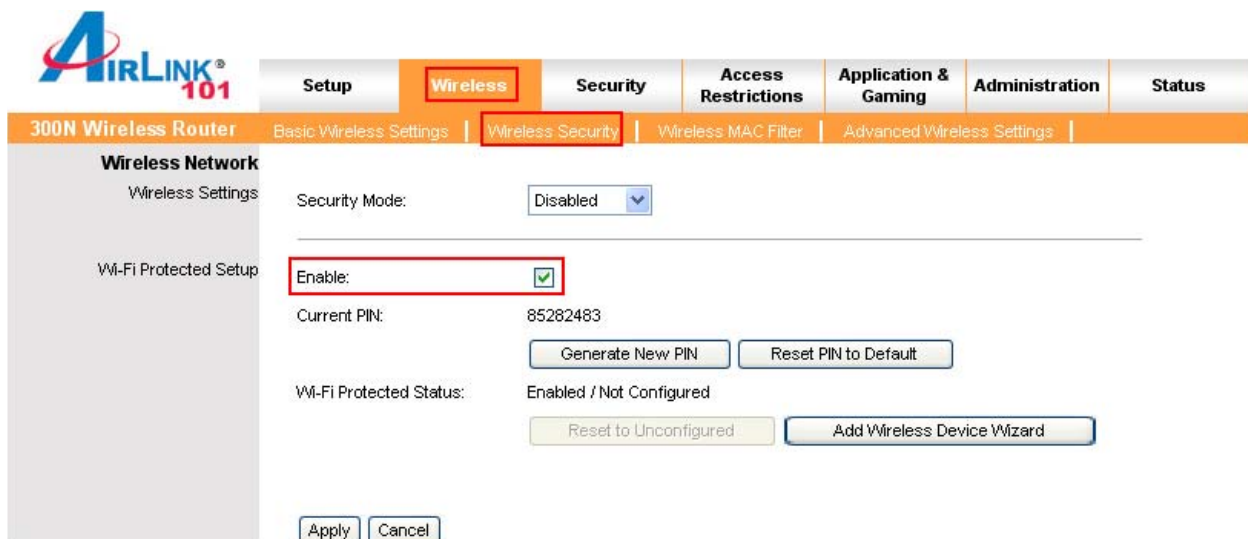
You have added the wireless device to your wireless network successfully, please click on the button below to continue.

Continue

Step 5 Click **Finish** on the WPS Connection screen.



Note: If you cannot connect successfully with WPS, you need to log in to your router's configuration and click on **Wireless**. Then click **Wireless security**. Make sure that the Wi-Fi Protected Setup **Enable** box is checked.



4.7 About

The About tab shows the Utility, Driver versions, and the MAC address of the adapter.



Appendix A – Features

Frequency Band

- 2.4~2.5 GHz

Standards

- IEEE 802.11b / 802.11g
- 802.11n draft 2.0

Interface

- PCI

Antenna type

- 3 external 2dBi antenna

Security

- WPA-PSK (TKIP)
- WPA2-PSK (AES)

Transmitted Power

- 802.11b: 17 dBm
- 802.11g: 14 dBm
- Draft 11n: 14 dBm

Data Rate

- Transmitting: Up to 300Mbps*
- Receiving: Up to 300Mbps*

System Requirements

- 150 MHz processor or better
- 64 MB RAM
- Available PCI slot

LEDs

- Activity
- Power

OS Compatibility

- Windows 2000/XP/Vista

Dimensions

- 234 x 122 x 23 mm (L x W)

Temperature

- Operating: 0°C to 55°C
- Storage: -20°C to 75°C

Humidity

- Operating: 10% to 80% Non-Condensing
- Storage: 5% to 90% Non-Condensing

Warranty

- Limited 1-year warranty

Safety Approvals

- FCC, CE, IC

Appendix B – Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- 1) this device may not cause interference and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Technical Support

E-mail: support@airlink101.com

Toll Free: 1-888-746-3238

Web Site: www.airlink101.com

*Theoretical maximum wireless signal rate derived from IEEE 802.11g standard and IEEE 802.11n draft specification version 2.0. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, mix of wireless products used, radio frequency interference (e.g., cordless telephones and microwaves) as well as network overhead lower actual data throughput rate. Specifications are subject to change without notice. All products and trademarks are the property of their respective owners. Copyright ©2008 AirLink101®